

CLAIMS

What is claimed is:

1. A method of authenticating the transaction via financing card, comprising steps of:

(a) issuing a financing card having an internal memory for storing the fingerprint of the card owner;

(b) reading out the fingerprint of the user through the fingerprint input device and referring the fingerprint data and the associated card number stored in said internal memory;

(c) authenticating the user by comparing said read-out fingerprint with said reference fingerprint data;

(d) referring a B/L database in order to check the credit status of said financing card when said authenticating step of (c) is passed; and

(e) approving a requested transaction when said credit-checking step of (d) is passed.

2. The method as set forth in Claim 1 wherein said internal memory is left blank at the issuing step of (a) and the fingerprint image is registered later in said internal memory through a fingerprint input device implement in an ATM.

3. A method of authenticating the transaction via financing card, comprising steps of:

(a) requesting a user to enter the pre-registered password in case when the operational mode for a third party's use is selected;

(b) requesting said user to input the fingerprint of said user's thumb once the entered password coincides with the pre-registered password at step (a);

(c) storing the fingerprint of said user at a memory of the ATM and referring to the B/L database for checking the credit status; and

(d) approving the requested transaction and printing the personal information of said user including the fingerprint on the transaction slip.

4. A system of authenticating the transaction via financing card, comprising:
- a fingerprint-registered financing card;
 - a server of a card company performing the procedures for the issuance of said fingerprint-registered financing card;
 - a card reader requesting a user to input the user's fingerprint and checking the authenticity by referring the reference fingerprint and B/L database;
 - an ATM processing said requested transaction and taking the fingerprint image of the user;
 - a server of a financial institution, connected to said server of a card company, communicating data including the fingerprint information with said ATM; and
 - a VAN performing network service for referring the B/L database or the fingerprint data.

5. The system as set forth in Claim 4 wherein said card reader further comprises a fingerprint input device and a processor for reading out the fingerprint of the user and comparing the read-out fingerprint with the reference fingerprint image.

6. The system as set forth in Claim 4 wherein said server of a card company further comprises:

- a B/L database storing a list of persons having poor credit status; and
- a membership database that stores personal including the fingerprint.

7. The system as set forth in Claim 4 wherein said server of a card company further comprises a web server connecting:

- a client computer having a card reader or a fingerprint input device;
- a card terminal having a fingerprint input device;
- a card company's server; or
- a financial institution's server.

8. The system as set forth in Claim 4 wherein said card reader comprises either a wired fingerprint-capturing device or a wireless fingerprint-capturing device.

9. The system as set forth in Claim 4 wherein said card reader further comprises an external interface module for reading out the fingerprint to the traditional credit card transaction device.